A Novel Approach for Survivability of IEEE 802.11 WLAN Against Access Point Failure

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF

Master of Technology

in

Computer Science and Engineering

(Specialization : Computer Science)

By

Manmath Narayan Sahoo

Department of Computer Science and Engineering
National Institute of Technology, Rourkela
Orissa-769008, India

2009

A Novel Approach for Survivability of IEEE 802.11 WLAN Against Access Point Failure

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF

Master of Technology

in

Computer Science and Engineering

(Specialization : Computer Science)

By

Manmath Narayan Sahoo

Under the Guidance of

Prof. Pabitra Mohan Khilar

Department of Computer Science and Engineering
National Institute of Technology, Rourkela
Orissa-769008, India

2009

To my family

NATIONAL INSTITUTE OF TECHNOLOGY
ROURKELA – 769008, ORISSA
INDIA

CERTIFICATE

This is to certify that the work in the thesis entitled **"A Novel Approach for Survivability of IEEE 802.11 WLAN Against Access Point Failure"** by **Mr.Manmath Narayan Sahoo** is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in the specialization of Computer Science in the department of Computer Science and Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Date: 26th May 2009

Place: NIT, Rourkela

Prof. Pabitra Mohan Khilar
Dept. of Computer Science and Engineering
National Institute of Technology
Rourkela – 769008

Acknowledgements

Before presenting the thesis work, I would like to mention a few words for the people who gave their unending support without which I would not have been able to complete my thesis entitled, **"A Novel Approach for Survivability of IEEE 802.11 WLAN Against Access Point Failure".**

My first thanks are to the Almighty God, without whose blessings I wouldn't have been writing this "acknowledgments".

With my sincere gratitude, I acknowledge the guidance, support and constant encouragement rendered by prof. Pabitra Mohan Khilar during the course of my master study at the National Institute of Technology, Rourkela. I am especially indebted to him for teaching me both research and writing skills, which have been proven beneficial for my current research and future career. Without his endless efforts, knowledge, patience, and answers to my numerous questions, this research would have never been possible.

I am very much indebted to Dr. B. Majhi, Head of the Department, Computer Science engineering, NIT Rourkela for his endless support during my work.

I am also grateful to Dr. A. K. Turuk, Dr. S. K. Rath, Dr. S. K. Jena, Dr. D. P. Mohapatra, Dr. R. Baliarsingh, Dr. B. D. Sahoo for their insightful feedback and encouragement which helped me to improve the presentation of the thesis in many ways.

I am also thankful to all the members of the Department of Computer Science and Engineering, and the Institute, for providing me with the necessary facilities and assistance in preparing the thesis work.

Finally, I thank all my family members and friends, who provided me constant moral support and stood by me throughout the duration of my M.Tech course.

Manmath Narayan Sahoo

Dissemination

[1] Manmath Narayan Sahoo, Pabitra Mohan Khilar, *"Survivability of IEEE 802.11 Wireless LAN Against AP Failure"*, International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), pp.424-428, April, 2009.

[2] Manmath Narayan Sahoo, Pabitra Mohan Khilar, "*System Level Fault Diagnosis in Distributed System"*, National Conference on Modern Trends of Operating Systems, pp.23-27, March, 2009.

Abstract

In the last decade, wireless networks have become increasingly popular as powerful and cost-effective platforms for mobile communications. Unfortunately, current wireless networks are notoriously prone to a number of problems, such as the loss of link-level connectivity due to user mobility and/or infrastructural failures, which makes it difficult to guarantee their reliability. Today's users are mostly satisfied with the ability to access wired networks/resources conveniently from mobile stations, even if the access is unreliable. However, as wireless networks become more ubiquitous and start to support more critical applications, users will expect wireless networks to provide the same guarantees of reliability as their wired counterpart are often able to ensure. Research is ongoing to extend the scope of services made available to mobile users to achieve the "anytime, anyplace, any form" communications vision. This vision is to provide voice, data, and multimedia services to users regardless of location, mobility pattern, or type of terminal used for access.

In IEEE 802.11 Wireless LAN, if an access-point fails, then, all the mobile stations connected to a wired network via the access-point may lose connectivity. In this thesis work, the problem of enhancing the survivability of IEEE 802.11 WLAN focusing on tolerating Access Point (AP) failures is addressed. In particular, focus on the problem of overcoming these APs failures working with reconfiguration of the remaining APs by changing parameters like the neighboring AP's MAC address is done. This approach consists of two main phases: Design and Fault Response. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of the active APs in order to deal with AP fault in the service area.

Contents

List of Figures

List of Tables

List of Acronyms

WLAN	Wireless Local Area Network
AP	Access Point
UAP	Universal Access Point
WDA	Wireless Distributed System
PDA	Personal Digital Assistants
BSS	Basic Service Set
IBSS	Independent Basic Service Set
ESS	Extended Service Set
SSID	Service Set IDentifier
MAC	Medium Access Control
WEP	Wired Equivalent Privacy
LLC	Logical Link Control
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
CS/CCA	Carrier Sense/Clear Channel Assessment
NIC	Network Interface Card
CRC	Cyclic Redundancy Check
PCS	Personal Communication Service

Chapter 1
Introduction

Chapter

1 Introduction

Wireless networks have been growing rapidly in the past years to support increasing demands for mobile communications. Though wired LAN provides sophisticated features to share resources and to have reliable communication among different nodes, sometimes it becomes a nightmare to physically connect several nodes located at different locations which are quite apart from each other. In such situation we need some other means of connecting those nodes. In this regard the Wireless Distributed System (WDS) features allow us to create large wireless networks by linking several wireless access points with WDS links. Thus WDS is normally used in large, open areas where pulling wires is cost prohibitive, restricted or physically impossible.

In IEEE 802.11 terminology a "Distribution System" [8] is system that interconnects so-called Basic Service Sets (BSS). A BSS is best compared to a "cell", driven by a single Access Point. So a "Distribution System" connects cells in order to build a premise wide network which allows users of mobile equipment to roam and stay connected to the available network resources.

A WDS link can be a point-to-point link [3] in which an access point can be wirelessly connected to at most one other access point or it can be of point-to-multipoint type [3] in which an access point can be wirelessly connected to several other access points. The following figures depict the Point-to-Point WDS Link and Point-to-Multipoint WDS Link.

Point-to-Point WDS Link:

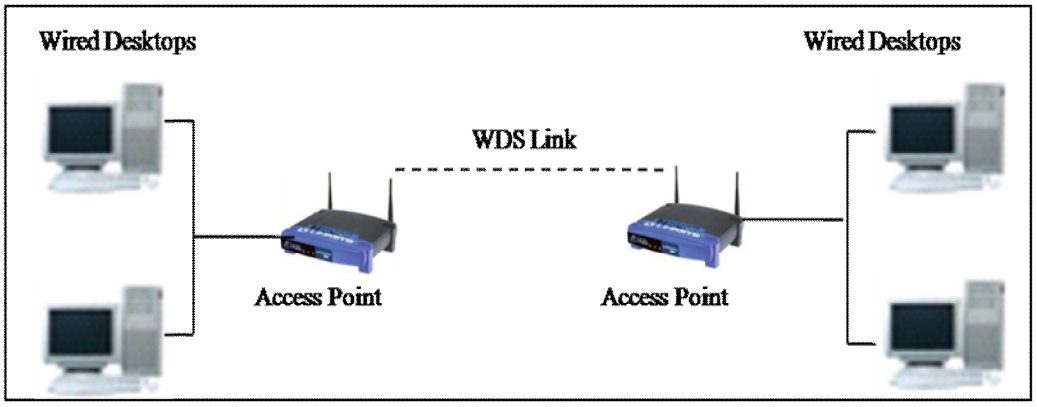

Figure 1.1. Point-to-Point WDS Link

Point-to-Multipoint WDS Link:

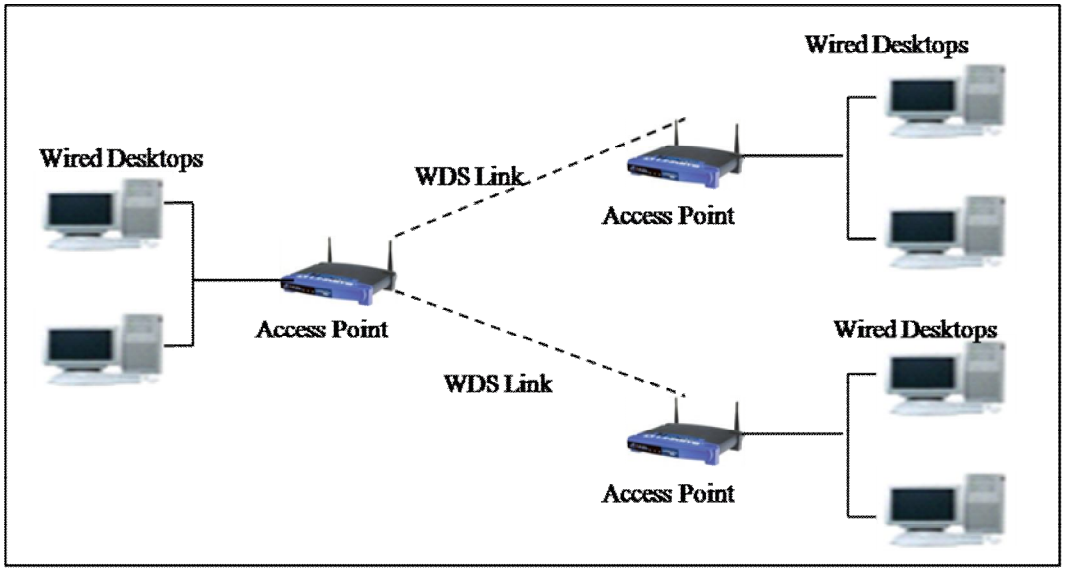

Figure 1.2. Point-to-Multipoint WDS Link

Wireless networks are increasingly being considered as the platform of choice for various applications. Critical applications, such as stock trading, health monitoring systems etc., require the underlying network to continue to function even in the presence of faults [1]. Unfortunately, current wireless networks are notoriously prone to a number of problems, such as the loss of link-level connectivity due to user mobility and/or infrastructural failures, which makes it difficult to guarantee their reliability. Today's users are mostly satisfied with the ability to access wired networks/resources conveniently from mobile stations, even if the access is unreliable. However, as wireless networks become more ubiquitous and start to support more critical applications, users will expect wireless networks to provide the same guarantees of reliability as their wired counterpart are often able to ensure. Research is ongoing to extend the scope of services made available to mobile users to achieve the "anytime, anyplace, any form" communications vision. This vision is to provide voice, data, and multimedia services to users regardless of location, mobility pattern, or type of terminal used for access.

In IEEE 802.11 Wireless Local Area Networks – WLANs, each AP has a coverage area, i.e., a limited range of operation, which is typically 20 to 300 meters in open

environments [1]. The IEEE 802.11 standard also provides for a handoff mechanism [5], in order to support the transfer of a mobile station from one AP to another, as the station moves between the respective coverage areas of the two APs. Thus, multiple APs are typically installed in order to provide seamless, continuous connectivity to mobile stations as they move from one location to another.

Though we take different measures to have smooth and reliable communication but in practice wireless network is more prone towards different types of errors such as such as the loss of link-level connectivity due to user mobility and/or infrastructural failures. For wireless (and wireline) networks, a network's ability to avoid or cope with failure is measured in three ways [2]:

- ***Reliability*** is a network's ability to perform a designated set of functions under certain conditions for specified operational times.
- ***Availability*** is a network's ability to perform its functions at any given instant under certain conditions. Average availability is a function of how often something fails and how long it takes to recover from a failure.
- ***Survivability*** is a network's ability to perform its designated set of functions given network infrastructure component failures, resulting in a service outage, which can be described by the number of services affected, the number of subscribers affected, and the duration of the outage.

1.1. WLAN Advantages

Wireless LANs offer users an array of benefits [9] ranging from cost efficiency to seamless integration with other networks.
The benefits of Wireless LANs include:

1. *Convenience*: Wireless freedom allows users to access network resources from any location. Even we can seat in our home and does our office work without any difficulty.
2. *Mobility*: Users move, but data is usually stored centrally, enabling users to access data while they are in motion can lead to large productivity gains. Networks are built because they offer valuable services to users. With the

emergence of public wireless networks, users can access the internet even outside their normal work environment.

3. *Productivity*: Using a PDA or any other wireless portable device, the user can remain constantly connected with the network.
4. *Deployment*: Many areas are difficult to wire for traditional wired LANs. Older buildings are often a problem; running cable through the walls of an older stone building to which the blueprints have been lost can be a challenge. In many places, historic preservation laws make it difficult to carry out new LAN installations in older buildings. Even in modern facilities, contracting for cable installation can be expensive and time-consuming. But initial setup of an infrastructure-based wireless network requires little more than an access point, as opposed to traditional networks which need wiring to be run to all locations.
5. *Expandability*: Adding additional clients to the network requires no additional infrastructure as long as they are within range because the network medium is already everywhere and there are no cables to pull, connect, or trip over.
6. *Cost*: Wireless networking hardware is only a slight cost increase from their wired counterparts, but the cost savings in infrastructure such as running cables, and expanding the network can offset this increase.

1.2. WLAN Disadvantages

Wireless LANs, despite the above mentioned advantages are still unpopular or an unconsidered option in many environments, this is due mostly to the inherent disadvantages [9] of the technology including:

1. *Security*: Security on any network is a prime concern. On wireless networks, it is often a critical concern because the network transmissions are available to anyone within range of the transmitter with the appropriate antenna. On a wired network, the signals stay in the wires and can be protected by strong physical-access control. On a wireless network, sniffing is much easier because the radio transmissions are designed to be processed by any receiver within range. Furthermore, wireless networks tend to have fuzzy boundaries. A corporate wireless network may extend outside the building. It is quite

possible that a parked car across the street could be receiving the signals from your network.

2. *Range*: The average range of an 802.11g network is approximately 30 meters; additional range requires either a repeater or additional access points.
3. *Reliability*: A wireless signal is susceptible to external interference, and thus the connection may become unstable, for this reason alone it is not recommended that important network resources such as servers be connected wirelessly.
4. *Speed*: The speed of wireless networks is constrained by the available bandwidth. 802.11g, the most common wireless network operates at 54Mbps, the most common wired networks operate at 100Mbps, with 1Gbps becoming increasingly common, and 10Gbps just emerging. Future wireless technologies such as 802.11n operate at 540Mbps greatly reducing the gap between wireless and wired speed.

1.3. Thesis Organization

Our research addresses the issues surrounding the survivability of wireless local area networks. In this thesis work, we propose a cost-effective mechanism to improve fault tolerance during access point failures in IEEE 802.11 WLAN. To clarify our work we need to specify what kind of AP faults this mechanism can recover. Initially, we are taking into account the occurrence of failures due to lack of energy to an AP or problems with the wired link to an AP. In particular, we focus on the problem of overcoming these AP's failures working with neighbor's MAC address and establishing a new path dynamically. Failures regarding to fault on AP functions or slighter problem (e.g., stops forwarding packets) or malfunction can't be detected and solved.

The thesis is organized in the following way: **Chapter 1** describes wireless LAN with its advantages and disadvantages. In **Chapter 2**, we have discussed various components of wireless LAN, different wireless LAN configuration techniques followed by traffic flow in wireless LAN. C**hapter 3** discusses IEEE 802.11 network services and mobility supports along with 802.11 layer descriptions. **Chapter 4** gives the overview of related work in this area. In **Chapter 5** we discuss our proposed work

along with simulation result. Finally, **Chapter 6** summarizes the main contributions of this thesis and comments on future directions for this research.

Chapter 2

Wireless LAN Architechture

Chapter 2

Wireless LAN Architecture

2.1. The Architecture

Various components of Wireless LAN are depicted in figure 2.1 and are described below.

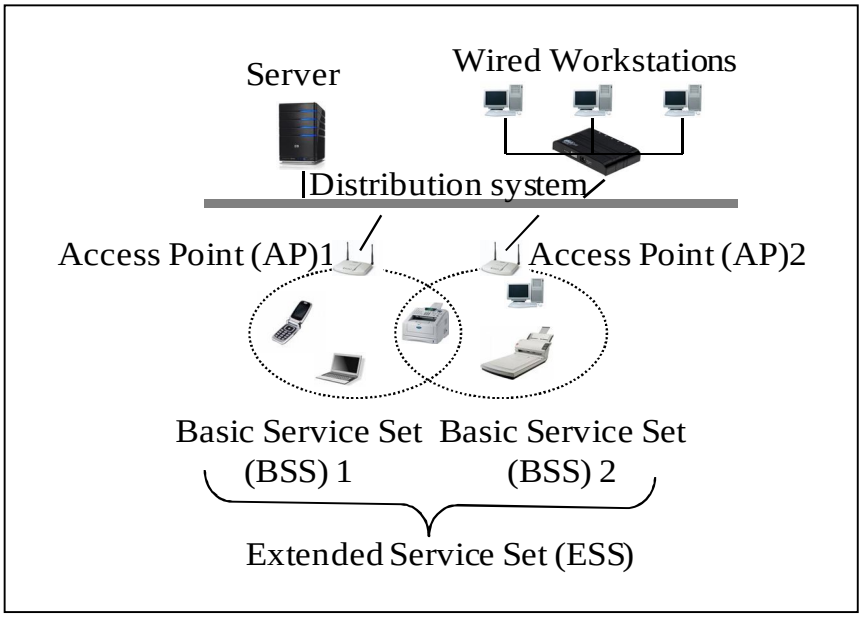

Figure 2.1. WLAN Architecture (Adapted form [9])

2.1.1. Stations

Networks are built to transfer data between stations. All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface cards (WNICs). Typically, stations are battery-operated laptop or handheld computers. Wireless Stations fall into one of two categories [9]: Access Points and Wireless Clients.

- *Access Points* (APs) are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.
- *Wireless Clients* can be mobile devices such as laptops, personal digital assistants (PDAs), IP phones or fixed devices such as desktops and workstations that are equipped with a wireless network interface card.

2.1.2. Basic Service Set

The basic building block of an 802.11 network is the basic service set (BSS), which is simply a group of stations that communicate with each other. Communications take place within a somewhat fuzzy area, called the basic service area. BSSs come in two flavors [9,12]: Independent BSS (also referred to as IBSS) and Infrastructure BSS. Every BSS has an id called BSSID; it is the MAC address of the Access Point servicing the BSS.

Stations in an IBSS communicate directly with each other and thus must be within direct communication range. The smallest possible 802.11 network is an IBSS with two stations. Typically, IBSSs are composed of a small number of stations set up for a specific purpose and for a short period of time. One common use is to create a short-lived network to support a single meeting in a conference room. As the meeting begins, the participants create an IBSS to share data. When the meeting ends, the IBSS is dissolved. Due to their short duration, small size, and focused purpose, IBSSs are sometimes referred to as *ad hoc BSSs* or *ad hoc networks*.

On the right side of Figure 2.2 is an infrastructure BSS. (To avoid overloading the acronym, an infrastructure BSS is never called an IBSS). Infrastructure networks are distinguished by the use of an access point. Access points are used for all communications in infrastructure networks, including communication between mobile nodes in the same service area.

If one mobile station in an infrastructure BSS needs to communicate with a second mobile station, the communication must take two hops. First, the originating mobile station transfers the frame to the access point. Second, the access point transfers the frame to the destination station. With all communications relayed through an access point, the basic service area corresponding to an infrastructure BSS is defined by the points in which transmissions from the access point can be received.

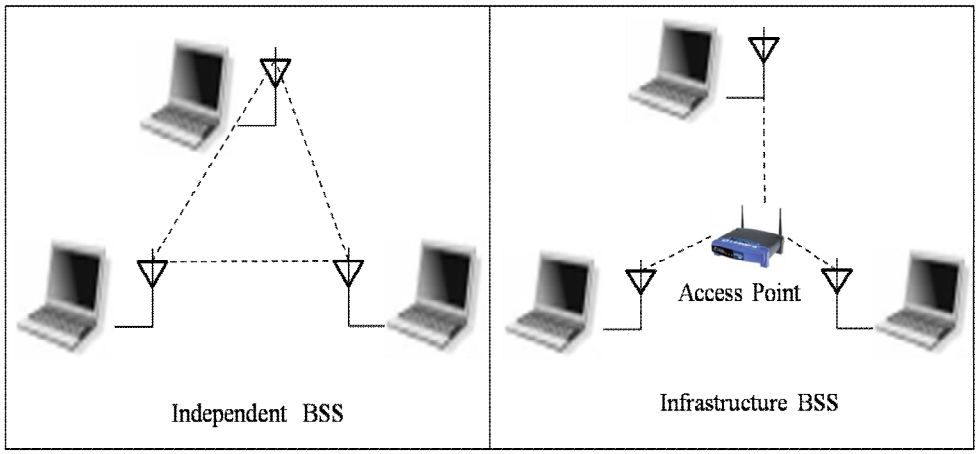

Figure 2.2. Independent and infrastructure BSSs (Adapted from [12])

Although the multi-hop transmission takes more transmission capacity than a directed frame from the sender to the receiver, it has two major advantages:

- An infrastructure BSS is defined by the distance from the access point. All mobile stations are required to be within reach of the access point, but no restriction is placed on the distance between mobile stations themselves. Allowing direct communication between mobile stations would save transmission capacity but at the cost of increased physical layer complexity because mobile stations would need to maintain neighbor relationships with all other mobile stations within the service area.
- Access points in infrastructure networks are in a position to assist with stations attempting to save power. Access points can note when a station enters a power-saving mode and buffer frames for it. Battery-operated stations can turn the wireless transceiver off and power it up only to transmit and retrieve buffered frames from the access point.

2.1.3. Extended Service Set

BSSs can create coverage in small offices and homes, but they cannot provide network coverage to larger areas. 802.11 allow wireless networks of arbitrarily large size to be created by linking BSSs into an extended service set (ESS) [13]. An ESS is

created by chaining BSSs together with a backbone network. All the access points in an ESS are given the same service set identifier (SSID), which serves as a network "name" for the users.

A *service set identifier or SSID* [10]**,** is a name used to identify the particular 802.11 WLAN to which a user wants to attach i.e. It distinguishes one WLAN from other. Thus multiple access points which are part of same network share the same SSID. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to, or by displaying a list of SSIDs in range and asking the user to select one. Example: Linksys (the default SSID for Linksys routers).

2.1.4. Distribution System

When several access points are connected to form a large coverage area, they must communicate with each other to track the movements of mobile stations. Thus the distribution system [13] provides mobility by connecting access points. When a frame is given to the distribution system, it is delivered to the right access point and relayed by that access point to the intended destination. The distribution system is responsible for tracking where a station is physically located and delivering frames appropriately. When a frame is sent to a mobile station, the distribution system is charged with the task of delivering it to the access point serving the mobile station. A distribution system is usually a wired LAN but also can be a wireless LAN.

2.1.5. Wireless Distribution System

When it is difficult to connect all of the Access Points in a network by wires, wireless interconnection of access points in an IEEE 802.11 network is required and in that case the distribution system is called as a *Wireless Distributed System* [9]. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required.

2.2. Advanced configurations

The flexibility that WDS offers, can yield numerous different configurations, those are described below.

2.2.1. Star configuration

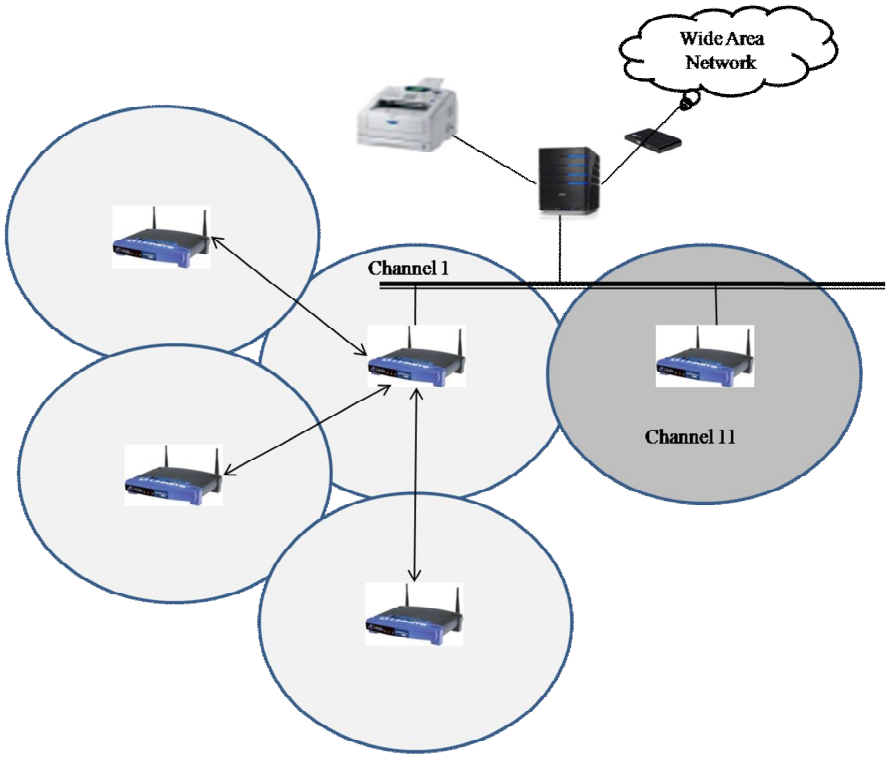

Figure 2.3. WLAN-Star configuration (Adapted from [8])

In a star configuration [8] WDS links are established between one AP and several others, as illustrated by the picture above. The central AP could be part of a wired infrastructure network, while the “satellite” APs are positioned to cover an area which is larger than can be covered by a single cell.

In this set-up the root AP needs three WDS ports enabled for 3 different links while the three satellites each have one WDS port enabled. It is not required that the port-index number assigned to a given WDS link is the same as the port-index number on the other side of the WDS link. In other words at the root AP, the MAC addresses for the three satellites are assigned to ports 3, 4 and 5, while in the satellite APs the MAC address of the root-AP can be entered in any port position that is available**.**

2.2.2. Chain configuration

Where the Star configuration can cover a more rectangular or square area, a Chain configuration [8] allows coverage of a longer shape (for instance a long corridor). The AP's are chained together, where the first AP for example could have a connection to the existing infrastructure (with all the network resources).

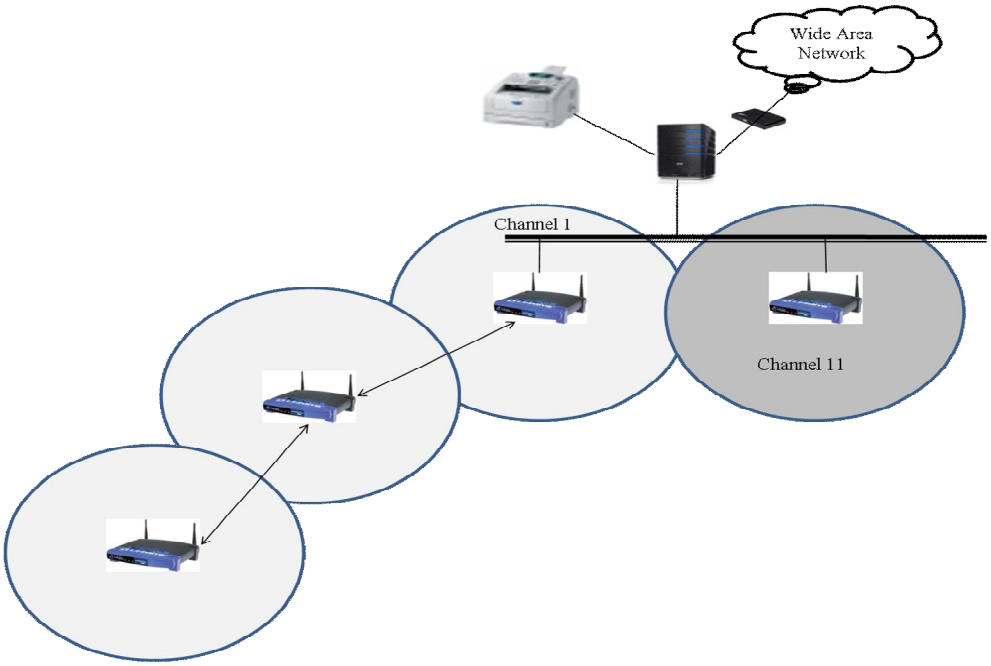

Figure 2.4. WLAN-Chain configuration (Adapted from [8])

In this setup the AP's at either end of the chain will need one WDS port enabled while the AP's in the middle of the chain will require two WDS ports to be configured to point upward and downward in the chain.

2.3. How does it work?

2.3.1. Addresses.

LAN devices (including wireless LAN devices) communicate which each other by using MAC addresses (which are hardware addresses uniquely assigned in the factory to each device). Each Wireless PC Card therefore has a unique MAC address that is used by the system to send data frames to it. All data frames transmitted over a LAN will contain a Destination and a Source MAC address as part of the frame header. If a data frame is transmitted over an Ethernet cable just those two MAC addresses are required. When data frames are to be transmitted between LAN end-stations that are

not connected to the same LAN segment, an intermediate device is required to "bridge" the frame from one segment to another. An access point is such a device also known as a bridge that has the capability to relay traffic from one segment to another. It performs this task with the use of a "*bridge learn table*" [8], where MAC addresses are stored in association with the LAN segment (or physical interface) where they reside.

Traffic between wireless LAN devices that conform to the IEEE 802.11 standard requires 4 MAC addresses instead of 2. When a wireless device is associated to an access point it will always direct its traffic to the access point by using the MAC address of the PC card in the access point as its direct destination address. The MAC address of the end station to which the frame was to be sent to is also included in the frame header, so that the PC card in the access point can determine where to relay the frame to. Finally the sending station's own MAC address is in the frame as the source address. So a total of three addresses are used.

When a WDS link is set up between two access points, all four available address fields in the MAC header are used:

- the MAC address of the sender,
- the MAC address of the final destination,
- the MAC address of the sending PC card in the access point,
- MAC address of the receiving PC card in the other access point.

2.3.2. Traffic Flow

In figure 2.5 Station1 (STA-1) in the left cell wants to transmit a frame to Station 2 (STA-2) in the right hand cell. The stations are associated to their respective access points, and are known in the bridge learn tables. Their MAC addresses "xxx" and "yyy" respectively are recorded in the bridge learn tables and related to a so called port number.

The steps in the traffic flow now are as follows [8]:

1. STA-1 sends its frame to the PC Card of its AP (because all its traffic goes in that direction); the frame includes the MAC address of the final destination, i.e. STA-2.

2. The PC Card in the left hand access point receives the traffic and acknowledges its correct reception to STA-1, converts the frame from an IEEE 802.11 format (with four addresses) to IEEE 802.3 format (Ethernet frame with two addresses, being the address of STA-1 as sender and STA-2 as destination). The PC Card then passes the frame to the AP-2000 bridge code.

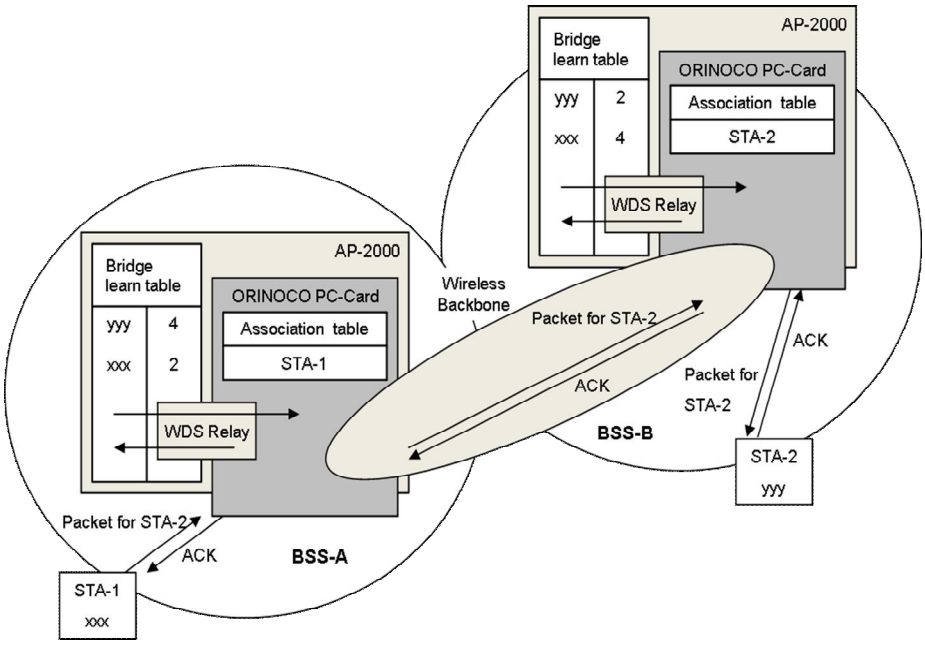

Figure 2.5. The traffic flow in WLAN (Adapted from [8])

3. The bridge code looks up the address of STA-2 in its bridge learn table and concludes that STA-2 is related to port 4. So the frame is passed on to the PC Card with the indication it is to be transmitted on port 4.

4. The PC Card itself maintains a table with the MAC addresses of the opposite end stations of the WDS links that it supports, so based on the port number the PC card will know the MAC address of the PC Card in the other AP.

5. The PC Card in the left-hand AP will now use the MAC address of the PC Card in the other AP as destination address, its own MAC address as source address, and will add the two addresses that were in the original frame received from the bridge. So now a total of 4 addresses are in the frame header.

6. The frame is transmitted on through the air and the PC Card in the other AP will receive the frame, send an acknowledgement back, convert the frame to a 2-address frame and passes it to its bridge.

7. The bridge will consult its bridge table, and passes the frame on to the PC card with indication to send it on port 2, being the BSS (cell) where the STA-2 is known to be.

8. Finally STA-2 accepts the frame and sends an acknowledgement back to the PC Card in the AP.

Chapter 3

802.11 Network Services and Mobility

Chapter 3 802.11 Network Services and Mobility

3.1. IEEE 802.11 Services

One way to define a network technology is to define the services it offers and allow equipment vendors to implement those services in whatever way they see fit. 802.11 provide eleven services [12]. Only three of the services are used for moving data; the remaining eight are management operations that allow the network to keep track of the mobile nodes and deliver frames accordingly. The services are described in the following list and summarized in Table I.

1. *Distribution:* This service is used by mobile stations in an infrastructure network every time they send data. Once a frame has been accepted by an access point, it uses the distribution service to deliver the frame to its destination. Any communication that uses an access point travels through the distribution service, including communications between two mobile stations associated with the same access point.

2. *Integration:* Integration is a service provided by the distribution system; it allows the connection of the distribution system to a non-IEEE 802.11 network.

3. *Association:* Delivery of frames to mobile stations is made possible because mobile stations register, or associate, with access points. The distribution system can then use the registration information to determine which access point to use for any mobile station. Unassociated stations are not "on the network," much like workstation with unplugged Ethernet cables.

4. *Reassociation:* When a mobile station moves between basic service areas within a single extended service area, it must evaluate signal strength and perhaps switch the access point with which it is associated. Reassociations are initiated by mobile stations when signal conditions indicate that a different association would be beneficial; they are never initiated directly by the access point. After the reassociation is complete, the distribution system updates its

location records to reflect the reachability of the mobile station through a different access point.

5. *Disassociation:* To terminate an existing association, stations may use the disassociation service. When stations invoke the disassociation service, any mobility data stored in the distribution system is removed. Once disassociation is complete, it is as if the station is no longer attached to the network. Disassociation is a polite task to do during the station shutdown process.

6. *Authentication:* Physical security is a major component of a wired LAN security solution. Network attachment points are limited, often to areas in offices behind perimeter access control devices. Network equipment can be secured in locked wiring closets, and data jacks in offices and cubicles can be connected to the network only when needed. Wireless networks cannot offer the same level of physical security, however, and therefore must depend on additional authentication routines to ensure that users accessing the network are authorized to do so. Authentication is a necessary prerequisite to association because only authenticated users are authorized to use the network. Authentication may happen multiple times during the connection of a client to a wireless network. Prior to association, a station will perform a basic identity exchange with an access point consisting of its MAC address. This exchange is often referred to as "802.11" authentication.

7. *Deauthentication:* Deauthentication terminates an authenticated relationship. Because authentication is needed before network use is authorized, a side effect of deauthentication is termination of any current association.

8. *Confidentiality:* Strong physical controls can prevent a great number of attacks on the privacy of data in a wired LAN. Attackers must obtain physical access to the network medium before attempting to eavesdrop on traffic. On a wired network, physical access to the network cabling is a subset of physical access to other computing resources. By design, physical access to wireless networks is a comparatively simpler matter of using the correct antenna and modulation methods. In the initial revision of 802.11, the confidentiality service was

called privacy, and provided by the now-discredited Wired Equivalent Privacy (WEP) protocol. In addition to new encryption schemes, 802.11i augments the confidentiality service by providing user-based authentication and key management services, two critical issues that WEP failed to address.

9. *MSDU delivery:* Networks are not much use without the ability to get the data to the recipient. Stations provide the MAC Service Data Unit (MSDU) delivery service, which is responsible for getting the data to the actual endpoint.

10. *Transmit Power Control (TPC):* TPC is a new service that was defined by 802.11h. European standards for the 5 GHz band require that stations control the power of radio transmissions to avoid interfering with other users of the 5 GHz band. Transmit power control [16] also helps avoid interference with other wireless LANs. Range is a function of power; high transmit power settings make it more likely that a client's greater range will interfere with a neighboring network. By controlling power to a level that is "just right," it is less likely that a station will interfere with neighboring stations.

11. *Dynamic Frequency Selection (DFS)* [17]*:* Some radar systems operate in the 5 GHz range. As a result, some regulatory authorities have mandated that wireless LANs must detect radar systems and move to frequencies that are not in use by radar. Some regulatory authorities also require uniform use of the 5 GHz band for wireless LANs, so networks must have the ability to re-map channels so that usage is equalized.

Table I. IEEE 802.11Network Services

	Service Type	**Usage**
Distribution	Distribution	Service used in frame delivery to determine destination address in infrastructure networks

Integration	Distribution	Frame delivery to an IEEE 802 LAN outside the wireless network
Association	Distribution	Used to establish the AP which serves as the gateway to a particular mobile station
Reassociation	Distribution	Used to change the AP which serves as the gateway to a particular mobile station
Disassociation	Distribution	Removes the wireless station from the network
Authentication	Station	Establishes station identity (MAC address) prior to establishing association
Deauthentication	Station	Used to terminate authentication, and by extension, association
Confidentiality	Station	Provides protection against eavesdropping
MSDU delivery	Station	Delivers data to the recipient
Transmit Power Control (TPC)	Station/spectrum management	Reduces interference by minimizing station transmit power
Dynamic Frequency Selection (DFS)	Station/spectrum management	Avoids interfering with radar operation in the 5 GHz band

3.1.1. Station services

Station services are part of every 802.11-compliant station and must be incorporated by any product claiming 802.11 compliant. Station services **[**14,20**]** are provided by both mobile stations and the wireless interface on access points. Stations provide frame delivery services to allow message delivery, and, in support of this task, they may need to use the authentication services to establish associations. Stations may also wish to take advantage of confidentiality functions to protect messages as they traverse the vulnerable wireless link.

3.1.2. Distribution system services

Distribution system services [14,20] connect access points to the distribution system. The major role of access points is to extend the services on the wired network to the wireless network; this is done by providing the distribution and integration services to the wireless side. Managing mobile station associations is the other major role of the distribution system. To maintain association data and station location information, the distribution system provides the association, reassociation, and disassociation services.

3.1.3. Spectrum management services

Spectrum management services [12] are a special subset of station services. They are designed to allow the wireless network to react to conditions and change radio settings dynamically. Two services were defined in 802.11h to help meet regulatory requirements.

The first service, transmit power control (TPC), can dynamically adjust the transmission power of a station. Access points will be able to use the TPC operations to advertise the maximum permissible power, and reject associations from clients that do not comply with the local radio regulations. Clients can use TPC to adjust power so that range is "just right" to get to the access point. Digital cellular systems have a similar feature designed to extend the battery life of mobile phones. Lower transmit power also will have some benefit in the form of increased battery life, though the extent of the improvement will depend on how much the transmit power can be reduced from what the client would otherwise have used.

The second service, dynamic frequency selection (DFS), was developed mainly to avoid interfering with some 5 GHz radar systems in use in Europe. Although originally developed to satisfy European regulators, the underlying principles have been required by other regulators as well. DFS was a key to the U.S. decision to open up more spectrums in the 5 GHz band in 2004. DFS includes a way for the access point to quiet the channel so that it can search for radar without interference, but the most significant part of DFS is the way that it can reassign the channel on an access point on the fly. Clients are informed of the new channel just before the channel is switched.

3.2. Mobility Support

Wireless networking and mobility are intertwined concepts. Without mobility, wireless networking would not be particularly interesting. Mobility [13,19] means that applications just work, no matter where the computer is. Unfortunately, building a network that provides location-independent services requires a great deal of location-based configuration and knowledge. The IEEE 802.11 standard, therefore, provides a handoff mechanism, in order to support the transfer of a mobile station from one access-point to another, as the station moves between the respective coverage areas of the two access-points.

The handoff process refers to the sequence of steps followed jointly by the mobile station and the access-point in transferring the link-level connectivity from one access-point to another. The IEEE 802.11 standard allows mobile stations to be handed over from one access-point to another, when a station moves between the coverage areas of the two access points. However, before a mobile station can be handed over to a new access-point, the mobile station should be able to discover the new access-point. The IEEE 802.11 standard allows two modes by which a mobile station can detect the presence of an access-point.

- *Passive Scanning* - In this mode, a mobile station sweeps from channel-to-channel (the 802.11 standard defines 13 channels of 5MHz each) to detect the presence of Beacon frames which are periodically transmitted by the access-points. The Beacon frames contain all the information that is needed by a

mobile station to associate itself with the access-point. A mobile station can establish the presence of an access-point on a channel if it is able to detect a Beacon frame on that channel. The advantage of passive scanning is that the mobile station saves battery power because it does not have to transmit anything.

- *Active Scanning* - In this mode, a mobile station actively seeks out access-points by broadcasting Probe Request frames on every channel. An access-point that receives a Probe Request frame responds to the client by sending the Probe Response frame. The mobile station can establish the existence of an access-point on a channel if it receives the Probe Response frame on that channel. But in wireless environment an intruder may send a burst of probe request frames very quickly, each with different MAC address (MAC Spoofing) to simulate the presence of large number of scanning stations in the area, inducing a heavy workload on the AP, resulting a denial of service attack called as Probe Request Flooding [15] attack.

Once a mobile station has discovered access-points in an area, it has to choose an access-point with which to associate. The IEEE 802.11 mandates that a mobile station be associated with only one access-point at a given time. This allows the switches in the wired network to forward the messages meant for a mobile station only to the access-point that the mobile station is associated with. Before a mobile station can be associated with an access point, it has to authenticate itself to the access-point. After the access-point sends an acknowledgment verifying the mobile station's identity, the mobile station sends a re-association request to the new access-point. The mobile station is considered to be associated with the new access-point only after it receives a reassociation response from the new access-point. The total latency in the entire handoff process is the sum of the delay in the scanning process to detect an access-point, and the delay in authenticating and re-associating the mobile station with the new access-point.

3.3. 802.11 Layer Description

Figure 3.1 shows 802.11 layers. IEEE 802.11 contains first two OSI layers viz. Physical layer and data link layer. The physical layer is further divided into Physical layer convergence procedure (PLCP) sublayer and physical medium dependent (PMD) sublayer. The data link layer is also divided into logical link control (LLC) sublayer and medium access control (MAC) sublayer.

<table>
<tr><td rowspan="2">OSI Layer 2: Data Link</td><td>802.2 Logical Link Control (LLC)</td></tr>
<tr><td>802.11 Medium Access Control (MAC)</td></tr>
<tr><td rowspan="2">OSI Layer 1: Physical</td><td>Physical Layer Convergence Procedure (PLCP)</td></tr>
<tr><td>Physical Medium Dependent (PMD)</td></tr>
</table>

Figure 3.1. IEEE 802,11 Layers

3.3.1. PLCP Sublayer

The MAC layer communicates with the Physical Layer Convergence Protocol (PLCP) [12] sublayer via primitives (a set of “instructive commands” or “fundamental instructions”) through a service access point (SAP). When the MAC layer instructs it to do so, the PLCP prepares MAC protocol data units (MPDUs) for transmission. The PLCP minimizes the dependence of the MAC layer on the PMD sublayer by mapping MPDUs into a frame format suitable for transmission by the PMD. The PLCP also delivers incoming frames from the wireless medium to the MAC layer.

The PLCP appends a PHY-specific preamble and header fields to the MPDU that contain information needed by the Physical layer transmitters and receivers. The 802.11 standard refers to this composite frame (the MPDU with an additional PLCP preamble and header) as a PLCP protocol data unit (PPDU). The MPDU is also called

the PLCP Service Data Unit (PSDU), and is typically referred to as such when referencing physical layer operations. The frame structure of a PPDU provides for asynchronous transfer of PSDUs between stations. As a result, the receiving station's Physical layer must synchronize its circuitry to each individual incoming frame.

3.3.2. PMD Sublayer

Under the direction of the PLCP, the Physical Medium Dependent (PMD) [12] sublayer provides transmission and reception of Physical layer data units between two stations via the wireless medium. To provide this service, the PMD interfaces directly with the wireless medium (that is, RF in the air) and provides modulation and demodulation of the frame transmissions. The PLCP and PMD sublayers communicate via primitives, through a SAP, to govern the transmission and reception functions.

3.3.3. Physical Layer Operations

The general operation [12,21] of the various Physical layers is very similar. To perform PLCP functions, the 802.11 standard specifies the use of state machines. Each state machine performs one of the following functions:

- Carrier Sense/Clear Channel Assessment (CS/CCA)
- Transmit (Tx)
- Receive (Rx)

3.3.3.1. Carrier Sense/Clear Channel Assessment (CS/CCA)

Carrier Sense/Clear Channel Assessment is used to determine the state of the medium. The Physical layer implements the carrier sense operation by directing the PMD to check to see whether the medium is busy or idle. The PLCP performs the following sensing operations if the station is not transmitting or receiving a frame:

- *Detection of incoming signals* - The PLCP within the station will sense the medium continually. When the medium becomes busy, the PLCP will read in the PLCP preamble and header of the frame to attempt synchronization of the receiver to the data rate of the signal.

- *Clear channel assessment* - The clear channel assessment operation determines whether the wireless medium is busy or idle [18]. If the medium is idle, the PLCP will send a PHYCCA. Indicate primitive (with its status field indicating idle) to the MAC layer. If the medium is busy, the PLCP will send a PHYCCA.indicate primitive (with its status field indicating busy) to the MAC layer. The MAC layer can then make a decision on whether to send a frame.

3.3.3.2. Transmit (Tx)

Transmit (Tx) is used to send individual octets of the data frame. The transmit procedure is invoked by the CS/CCA procedure immediately upon receiving a PHY-TXSTART.request (TXVECTOR) from the MAC sublayer. The CSMA/CA protocol is performed by the MAC with the PHY PLCP in the CS/CCA procedure prior to executing the transmit procedure.

3.3.3.3. Receive (Rx)

Receive (Rx) is used to receive individual octets of the data frame. The receive procedure is invoked by the PLCP CS/CCA procedure upon detecting a portion of the preamble sync pattern followed by a valid SFD and PLCP Header. Although counter-intuitive, the preamble and PLCP header are not “received”. Only the MAC frame is “received”.

3.3.4. 802.11 MAC Layer Functions

The 802.11 MAC is the lower sublayer of the data link layer in the protocol stack. The following are the primary 802.11 MAC functions [21,22,12], especially as they relate to infrastructure wireless LANs:

- **Scanning**: The 802.11 standard defines both passive and active scanning; whereby, a radio NIC searches for access points. Passive scanning is mandatory where each NIC scans individual channels to find the best access point signal. Periodically, access points broadcast a beacon, and the radio NIC receives these beacons while scanning and takes note of the corresponding signal strengths. The beacons contain information about the access point, including service set identifier (SSID), supported data rates, etc. The radio

NIC can use this information along with the signal strength to compare access points and decide upon which one to use.

Optional active scanning is similar, except the radio NIC initiates the process by broadcasting a probe frame, and all access points within range respond with a probe response. Active scanning enables a radio NIC to receive immediate response from access points, without waiting for a beacon transmission. The issue, however, is that active scanning imposes additional overhead on the network because of the transmission of probe and corresponding response frames.

- **Authentication**: Authentication is the process of proving identity, and the 802.11 standard specifies two forms: Open system authentication and shared key authentication. Open system authentication is mandatory, and it's a two step process. A radio NIC first initiates the process by sending an authentication request frame to the access point. The access point replies with an authentication response frame containing approval or disapproval of authentication indicated in the Status Code field in the frame body.

  Shared key authentication is an optional four step process that bases authentication on whether the authenticating device has the correct WEP (wired equivalent privacy) key. The radio NIC starts by sending an authentication request frame to the access point. The access point then places challenge text into the frame body of a response frame and sends it to the radio NIC. The radio NIC uses its WEP key to encrypt the challenge text and then sends it back to the access point in another authentication frame. The access point decrypts the challenge text and compares it to the initial text. If the text is equivalent, then the access point assumes that the radio NIC has the correct key. The access point finishes the sequence by sending an authentication frame to the radio NIC with the approval or disapproval.

- **Association**: Once authenticated, the radio NIC must associate with the access point before sending data frames. Association is necessary to synchronize the radio NIC and access point with important information, such as supported data rates. The radio NIC initiates the association by sending an association request

frame containing elements such as SSID and supported data rates. The access point responds by sending an association response frame containing an association ID along with other information regarding the access point. Once the radio NIC and access point complete the association process, they can send data frames to each other.

- **WEP**: With the optional WEP enabled, the wireless NIC will encrypt the body (not header) of each frame before transmission using a common key, and the receiving station will decrypt the frame upon receipt using the common key. The 802.11 standard specifies a 40-bit key and no key distribution method, which makes 802.11 wireless LANs vulnerable to eavesdroppers. The 802.11i committee, however, is improving 802.11 securities by incorporating 802.1X and stronger encryption into the standard.

- **RTS/CTS**: The optional request-to-send and clear-to-send (RTS/CTS) function allows the access point to control use of the medium for stations activating RTS/CTS. With most radio NICs, users can set a maximum frame length threshold whereby the radio NIC will activate RTS/CTS. For example, a frame length of 1,000 bytes will trigger RTS/CTS for all frames larger than 1,000 bytes. The use of RTS/CTS alleviates hidden node problems, that is, where two or more radio NICs can't hear each other and they are associated with the same access point.

  If the radio NIC activates RTS/CTS, it will first send a RTS frame to access point before sending a data frame. The access point will then respond with a CTS frame, indicating that the radio NIC can send the data frame. With the CTS frame, the access point will provide a value in the duration field of the frame header that holds off other stations from transmitting until after the radio NIC initiating the RTS can send its data frame. This avoids collisions between hidden nodes. The RTS/CTS handshake continues for each frame, as long as the frame size exceeds the threshold set in the corresponding radio NIC.

- **Power Save Mode:** The optional power save mode that a user can turn on or off enables the radio NIC to conserve battery power when there is no need to send data. With power save mode on, the radio NIC indicates its desire to enter

"sleep" state to the access point via a status bit located in the header of each frame. The access point takes note of each radio NIC wishing to enter power save mode, and buffers packets corresponding to the sleeping station.

In order to still receive data frames, the sleeping NIC must wake up periodically (at the right time) to receive regular beacon transmissions coming from the access point. These beacons identify whether sleeping stations have frames buffered at the access point and waiting for delivery to their respective destinations. The radio NICs having awaiting frames will request them from the access point. After receiving the frames, the radio NIC can go back to sleep.

- **Fragmentation**: The optional fragmentation function enables an 802.11 station to divide data packets into smaller frames. This is done to avoid needing to retransmit large frames in the presence of RF interference. The bits errors resulting from RF interference are likely to affect a single frame, and it requires less overhead to retransmit a smaller frame rather than a larger one. As with RTS/CTS, users can generally set a maximum frame length threshold whereby the radio NIC will activate fragmentation. If the frame size is larger than the threshold, the radio NIC will break the packet into multiple frames, with each frame no larger than the threshold value.

3.3.5. 802.2 LLC Layer Functions

The LLC layer is responsible for [23,24,12]:

- Multiplexing (splitting multiple messages over one stream) protocols transmitted over the MAC layer and demultiplexing them (putting the messages back together)

- Providing flow and error control: The LLC multiplexes information by splitting it into 'frames' of data and sending the frames across the line, and arranging the frames back in order. The LLC specifies the order in which frames are to be assembled with a header, a tag of information that says what to do with the information that is sent once it is received.

- The LLC's other responsibility is to control errors. The LLC does this using a CRC, or Cyclic Redundancy Check. Each frame has a trailer that contains a few bits of information on how the information in that frame is to be put together. The receiving node compares the information in the trailer with the information that it has assembled, to see if they match up.

Chapter 4
Related Work

Chapter 4

Related Work

4.1. Access-Point Replication

One strategy to tolerate access-point failures in wireless networks is to use an additional access-point that is designated as a backup [5], and that can be activated once the primary (the previously operational) access-point fails. In this technique, the backup access-point must be able to detect the primary access-point's failure; also, as a part of fault-recovery, all of the mobile stations that were associated with the failed access-point must switch over to the backup access-point. Apart from the inherent latency involved in detecting access-point failures and performing the fail-over, this results in additional infrastructural costs – wireless service providers would now need to deploy additional access points which might not necessarily be actively used under fault-free conditions, but are nevertheless required for fault-recovery.

4.2. Overlapping-Coverage Approach

Another technique to tolerate access-point failures is to use access-points with overlapping coverage [5]. The principal idea in providing overlapping coverage across different access points is that, if one access-point fails, mobile stations associated with that access-point can be transferred over to another access-point whose coverage area intersects with that of the failed access-point.

Although this technique has been proposed to tolerate infrastructural failures in cellular networks, there are a number of technical difficulties in adopting this approach in 802.11 wireless networks. The IEEE 802.11 standard operates in the limited 2.4 GHz ISM (industrial, scientific and medical) band. The frequency band is further divided into 13 channels of 5 MHz each. Furthermore, the IEEE 802.11 standard mandates that the channels used by neighboring access-points be separated by at least five channels in order to minimize radio interference between the neighboring access-points. This restriction implies that there are only three channels available to construct an extended service set. Given that the number of channels to cover the extended service set is limited, it might not be possible to ensure that overlapping coverage is available everywhere.

Furthermore, the use of the overlapping-coverage scheme requires that some spare capacity be reserved at each access-point to take over the additional users that the access-point will have to support in case a neighbor access-point (with overlapping coverage) fails. If spare capacity is not provisioned, and all of the overlapping access points are loaded to their respective capacities when one of the access-points fail, then, the mobile stations associated with the failed access-point will cause the target throughput of users in the overlapping coverage area to decrease.

Another significant issue in using overlapping coverage to tolerate access-point failures is the latency involved in detecting an access-point failure and switching (through the handoff mechanism) to a functional access-point. If this delay is relatively large, then, a number of applications that require stringent bounds on the overall delay may not function properly (although some applications such as web browsers are relatively tolerant to long delays).

4.3. Multifunction/multimode devices

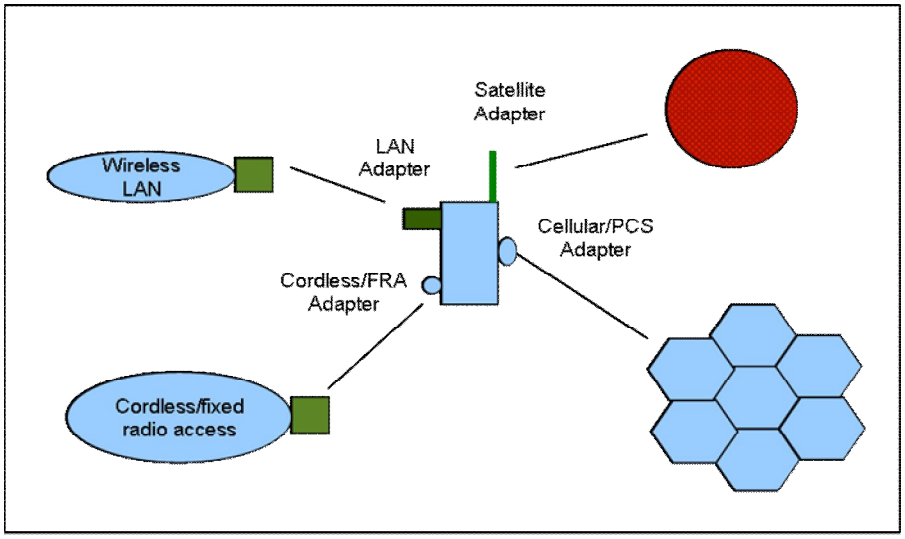

Figure 4.1. Using Multifunction/Multimode devices to increase Survivability (Adapted from [2])

Another way to improve survivability is to use multifunction/ multimode devices [2] in which a single terminal offers multiple interfaces, as shown in the figure 4.1. Early examples of this architecture include the dual function advanced mobile phone system (analog cellular)/ code division multiple access (PCS standard) satellite/cell

phone, the emerging group system for mobile communications, and Digital Enhanced Cordless Telephony, the European PCS standard. This architecture provides overlapped services to ensure wireless coverage in case of network, link, or switch failure. It may also increase the effective coverage area.

4.4. Overlay Network

Yet another way to improve survivability and hide network failure is to deploy an overlay network [2]. As Figure 4.2 shows, in this architecture, a user accesses an overlay network consisting of several universal access points, which choose a wireless network for the user based on availability, specified quality of service, and user-specified choices. A universal access point performs protocol and frequency translation, as well as content adaptation. All of these techniques involve capital investment. It is up to each carrier to evaluate the trade-off between the increased expenditures and customer satisfaction— a difficult decision- making process that will become more necessary in the future as dependence on wireless grows.

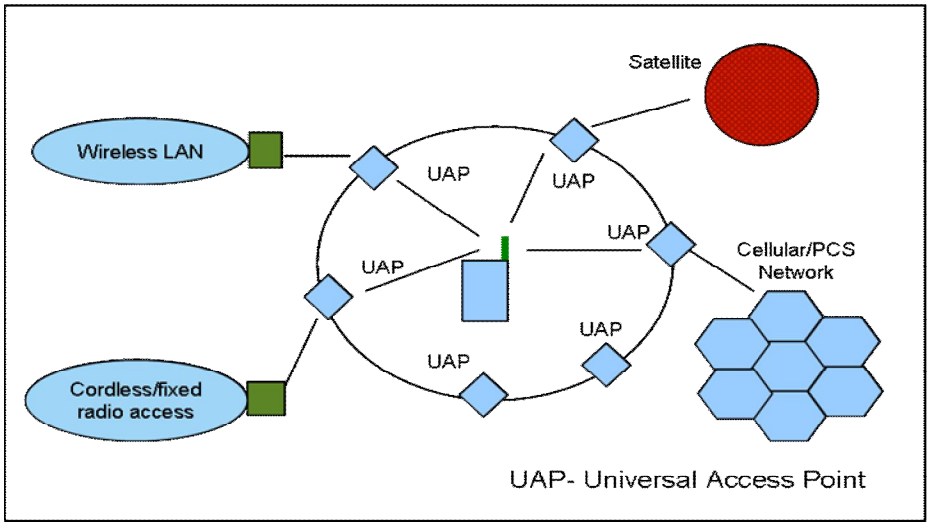

Figure 4.2. Using Overlay network to increase Survivability (Adapted from [2])

Hass et al. [6] describe a technique to tolerate the failure of the location database, which is a repository of the locations of mobile stations at the mobile switching centers in PCS network. Chen et al. [11] describe a scheme for enhancing the connection reliability in WLANs by tolerating the existence of *shadow regions* through placement of redundant APs. But the presence of redundant APs, may lead to

co-channel interference problems. But our scheme is not based on redundancy and does not require shadow access points. Tipper et al. [4,7] present a survivability analysis of Personal Communication Service (PCS) networks. The results of their simulation model demonstrate that user mobility can significantly degrade the performance of the network, in the presence of failures.

Chapter 5

Proposed Model: Design and Implementation

Chapter 5 Proposed Model : Design and Implementation

A simple fault detection approach, based on response timeout, which promises to be more cost-effective to identify failures due to lack of energy to an AP or problems with the wired link to an AP is developed. In particular, focus on the problem of overcoming these APs failures working with reconfiguration of the remaining APs by changing parameters like the neighboring AP's MAC address is done. This approach consists of two main phases [25]: *Design* and *Fault Response*. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of the active APs in order to deal with AP fault in the service area.

5.1. Design Phase (Algorithm for Establishing Route)

Statement: This algorithm finds the minimum spanning tree and assigns redundant MAC IDs to each node of the minimum spanning tree for network survival in case of any AP failure.

Input:

- Location of access points (Latitude and Longitude),
- Range of the access points.

Output:

- MAC ID for establishing the network.
- Redundant MAC ID for network survivability.

The algorithm consists of 6 main steps which are described in figure 5.1.

Step 1. For 'n' nodes construct adjacency matrix A[n][n], where A[i[][j] represents the distance between the node i and j (Distance is calculated from latitude and longitude).Enter the threshold value 'T'.

Step 2. Update the adjacency matrix by comparing each element A[i][j].

If A[i][j] > T then, make A[i][j]=0,

as the nodes are not valid for being out of WiFi range.

Step 3. Find the minimum spanning tree from the matrix A[n][n].

Step 4. Apply BFS to the graph and store the traversing sequence in an array BFS[ ].

Step 5. Store adjacent node's MAC ID in each node of the spanning tree.

Each spanning tree node has an array Neighbor[ ] associated with it.

This array is used to store the MAC ID of the adjacent nodes in minimum spanning tree.

Step 6. Find valid redundant nodes for each node in BFS[] and insert valid MAC IDs.

For i=n-1 to 0 *continue*

For j=i-1 to 0 *continue*

If (BFS[j] is valid node for BFS[i]) *then*

Insert MAC ID of BFS[j] to the MAC ID array of BFS[i] only when the MAC ID is not previously present.

End if

End for

End for

Figure 5.1: Algorithm for establishing route

5.2. Fault Response Phase (Network Survivability Algorithm)

Statement: This algorithm is used to make the network survive in case of failure of any access point.

Input:

- The modified weight adjacency matrix of the network,
- The MAC ID list associated with each node,
- The minimum spanning tree generated by above algorithm.

Output:

- A connected network consisting of the remaining active APs.

The algorithm consists of 3 main steps which are described in figure 5.2.

Step 1. Apply DFS to the spanning tree and store the traversing sequence in an array DFS[ ].
Step 2. Find failure node (say F) applying ping between starting node and the node in DFS[ ].
Step 3.
For each adjacent node N of F in the spanning tree *continue*
Find the adjacency list L of node N from the modified weight adjacency matrix.
For each node in L *continue*
Store the MAC ID in N's Neighbor[ ] iff it is not already present and does not form a loop.
End for
End for

Figure 5.2. Network survivability Algorithm

5.3.Worked Out Example

Algorithm for Establishing Route

Step 1: The complete graph for 7 Access Points is shown in Figure 5.3 along with the initial weight adjacency matrix in Table II.

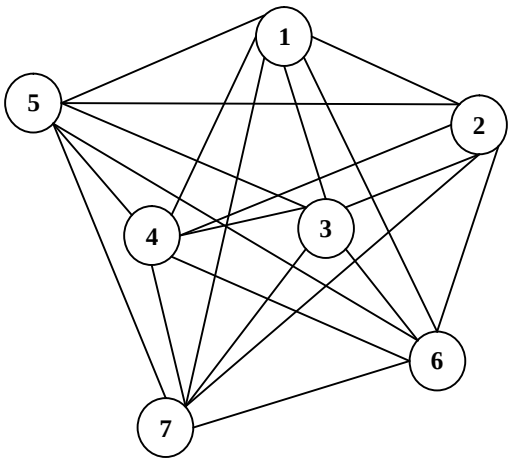

Figure 5.3. Complete graph for access point network.

TABLE II. INITIAL WEIGHT ADJACENCY MATRIX

	1	2	3	4	5	6	7
1	0	4	8	9	5	12	11
2	4	0	5	8	7	7	9
3	8	5	0	5	11	5	8
4	9	8	5	0	5	12	6
5	5	7	11	5	0	13	11
6	12	7	5	12	13	0	7
7	11	9	6	8	11	7	0

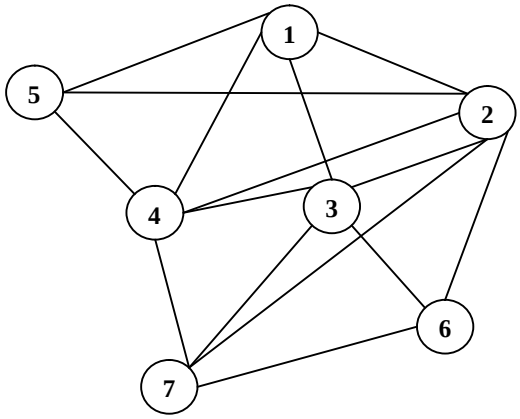

Figure 5.4. Modified graph after pruning against threshold value (T=9).

TABLE III. MODIFIED WEIGHT ADJACENCY MATRIX

	1	2	3	4	5	6	7
1	0	4	8	9	5	0	0
2	4	0	5	8	7	7	9
3	8	5	0	5	0	5	8
4	9	8	5	0	5	0	6
5	5	7	0	5	0	0	0
6	0	7	5	0	0	0	7
7	0	9	6	8	0	7	0

Step 2: Checking with the threshold value, T=9, the adjacency matrix is modified (shown in Table III) and the modified graph is found as shown in Figure 5.4

Step 3: Minimum spanning tree of the modified graph is depicted in Figure 5.5.

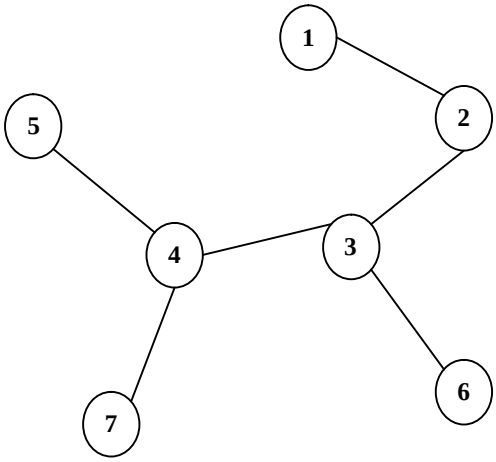

Figure 5.5. Minimum spanning tree of the modified graph.

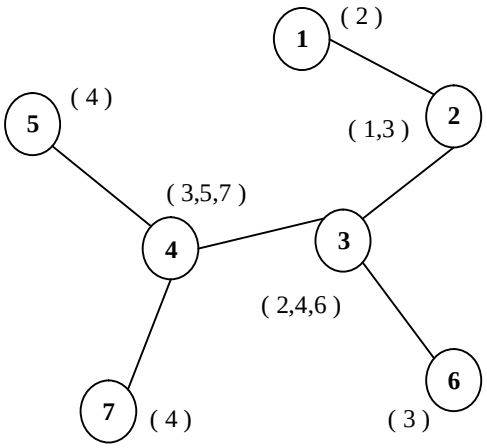

Figure 5.6. Access Points with neighbor MAC IDs

Step 4: The BFS traversal sequence of the graph is 1,2,5,3,4,6,7

Step 5: Figure 5.6 shows the initial neighborhood MAC ID assignments

Step 6: Figure 5.7 shows redundant MAC ID assignments to the minimum spanning tree.

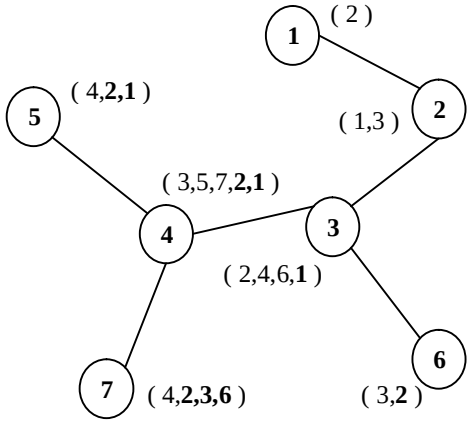

Figure 5.7. Access Points with neighbor and redundant MAC IDs

Network Survivability Algorithm

Step 1: Output of DFS traversal sequence of the minimum spanning tree is 1,2,3,4,5,7,6

Step 2: Ping to the access points in the DFS sequence.

Ping to AP 1: It is responding.

Ping to AP2: It is not responding.

Again ping to AP 1: It is responding.

This implies AP 2 has failed.

i.e. F=2

Step 3: The neighboring nodes of F (=2) are 1 and 3.

Adjacency list of AP 1 in DFS order: [3,4,5].

Adjacency list of AP 3 in DFS order: [1,4,7,6].

By placing 3 as the neighbor of 1 all the active APs become connected and it does not lead to loop formation.

By placing 4 or 5 as the neighbor of 1 leads to loop formation so we discard them.

By placing 7 as the neighbor of 3 leads to loop formation so we discard it, and node 1,4, and 6 are already in neighbor list of 3.

So step 3 stops and figure 5.8 shows the final network after survival.

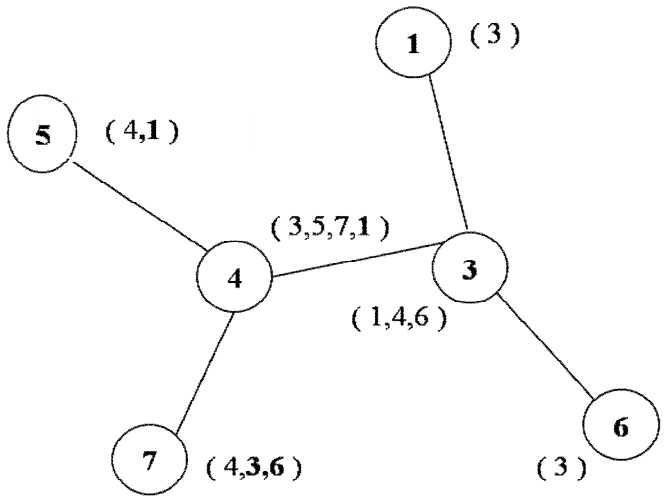

Figure 5.8. Final network after survival

5.4. Simulation and Results

In this section we present the results of our simulations, which we performed in *ns-2* to evaluate the efficiency of our algorithm. We tested our algorithm on a 3.0GHz processor, in linux (Ubuntu 8.04) environment and below we report the result of one such simulation scenario. To get each point in the graph we considered the average no of clock cycles for 10 executions of our algorithm for networks or different size and we have compared the result of this algorithm with our previous work in [25].

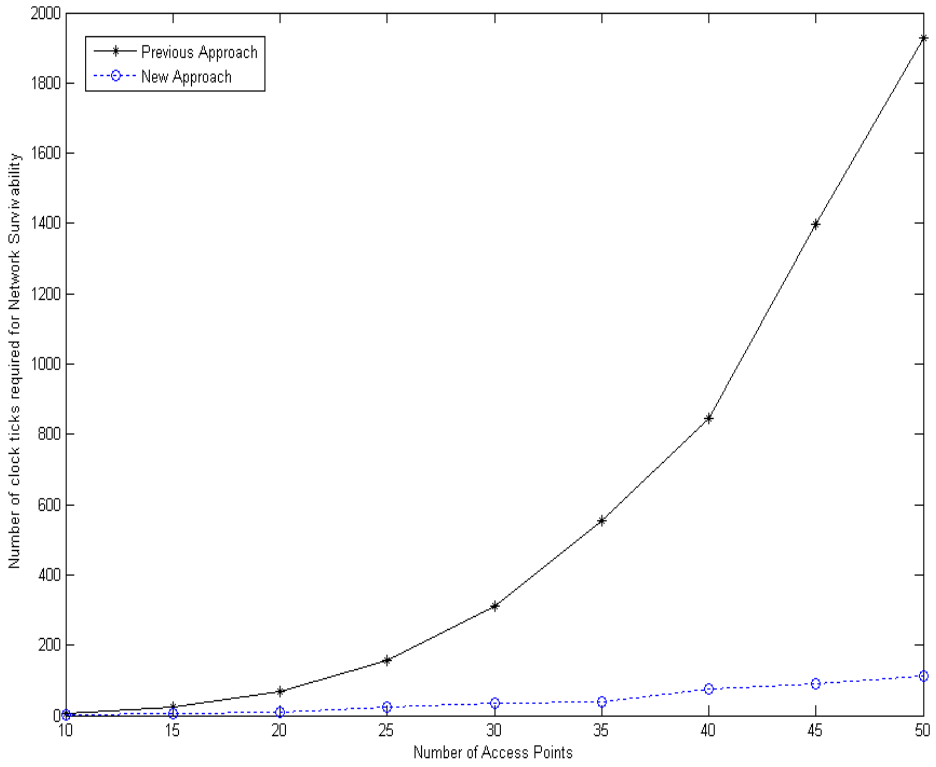

Figure 5.9. Variation of no of clock cycles required for network survivability w.r.t. Network size.

The graph in figure 5.9 depicts how the no of required clock cycles to maintain network connectivity in case of Access Point failure varies with respect to the change in network size i.e. with respect to the change in no of access points in wireless LAN. The dotted line shows the behavior of this algorithm and the solid line shows the behavior of the algorithm in our previous work [25]. The behavior of the graph implies that, as the network size increases with respect to the no of access points, no

of clock cycles required to maintain network connectivity in case of access point failure also increases. It is clear from the graph that, the growth rate of this algorithm is very low as compared to the algorithm proposed in [25]. The behavior is obvious because with the increase in no of APs, the size of the neighborhood list of a failed AP also increases thus step 3 of network survivability algorithm takes more no of clock cycles to complete its execution. Thus the no of clock cycles required not only depends on the no of APs but also on the network structure. Finally the graph shows that the performance of this approach is better than our previous work.

Chapter 6

Conclusion & Future Work

Chapter

6 Conclusion and Future Work

6.1. Summary of Thesis Work

Though we take different measures to make the wireless network more reliable, unfortunately, current wireless networks are notoriously prone to a number of problems, such as the loss of link-level connectivity due to user mobility and/or infrastructural failures, which makes it difficult to guarantee their reliability. The use of wireless network is so pervasive that now a day's users are least concerned about the reliability, they are more concerned about the ability to access wired networks/resources conveniently from mobile stations, even if the access is unreliable. But in some situations where the wireless network supports critical applications, reliability is a measure concern. In these cases the wireless network must able to provide the same level of reliability as their wired counterparts are often able to ensure.

In this thesis work, we have proposed a survivability scheme for IEEE 802.11 Wireless Local Area Network in case of AP failure. This algorithm can be used to make the network survive dynamically with the assumption that each Access Point must have place to hold the redundant MAC IDs of neighboring APs. A simple fault detection approach, based on response timeout, which promises to be more cost-effective to identify failures due to lack of energy to an AP or problems with the wired link to an AP is developed. In particular, focus on the problem of overcoming these APs failures working with reconfiguration of the remaining APs by changing parameters like the neighboring AP's MAC address is done. This approach consists of two main phases: Design and Fault Response. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of the active APs in order to deal with AP fault in the service area.

6.2. Future Research Direction

The proposed algorithm is designed to handle single access point failure at time, so the algorithm can be enhanced to handle multiple access point failure at a time and the performance of the algorithm can be compared with this approach. In this approach the set up of the network is done statically, the algorithm can be enhanced to incorporate dynamic set up of network. All the access points are given static IP addresses and this can be enhanced for dynamic IP addressing of the access points and the behavior of the algorithm can be studied with respect to the current approach after simulation. The algorithm can be enhanced by adding restoration of the previous configuration after the failed AP is corrected and restored.

Bibliography

[1] Flavio E. de Deus, Ricardo Staciarini Puttini, Luis Fernando Molinaro, Joseph Kabara; “On Survivability of IEEE 802.11 WLAN”; Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing; 2006.

[2] A. P. Snow, U. Varshney, and A. D. Malloy. “Reliability and survivability of wireless and mobile networks”. IEEE Computer, 49–55, July 2000.

[3] “Configuring a Wireless Distribution System (WDS) with the 3Com OfficeConnect Wireless 11a/b/g Access Point” [online]. Available:”www.3com.com/other/pdfs/products/en_US/104108.pdf”.

[4] D. Tipper, T. Dahlberg, H. Shin, and C. Charnsripinyo. “Providing fault tolerance in wireless access networks”. IEEE Communications, 62–68, January 2002.

[5] Rajeev Gandhi; “Tolerance to Access-Point Failures in Dependable Wireless Local-Area Networks”; Proceedings of the Ninth IEEE International Workshop on Object-Oriented Real-Time Dependable Systems; 2004.

[6] Z. J. Haas and Y.-B. Lin. “Demand re-registration for PCS database restoration”. Mobile Networks and Applications, 191–198, 2000.

[7] D. Tipper, S. Ramaswamy, and T. Dahlberg. “PCS network survivability”. Mobile and Wireless Communication Networks conference, September 1999.

[8] “WDS (Wireless Distribution System)”; ORiNOCO Technical Bulletin 046/ A; February 2002.

[9] Wireless Local Area Network (WLAN) Explained [online]. Available: http://www.anthonycairns.com/Explained/Items_Explained_WLAN.htm

[10] Service Set Identifier [online]. Available: http://wapedia.mobi/en/Service_set_identifier

[11] D. Chen, C. Kintala, S. Garg, and K. S. Trivedi. “Dependability enhancement for IEEE 802.11 wirelessLAN with redundancy techniques”. Proceedings of the International Conference on Dependable Systems and Networks, 521–528, June 2003.

[12] Matthew Gast, “802.11 Wireless Networks: The Definitive Guide”, O’Reilly Publication, April, 2005.

[13] Pablo Brenner, “A Technical Tutorial on the IEEE 802.11 Protocol”, Breezecom Wireless Communications, July, 1996.

[14] IEEE 802.11 Services [Online]. Available: http://www.informit.com/articles/article.aspx?p=24411&seqNum=7

[15] M. Bernaschi, F. Ferreri and L. Valcamonici, “Access points vulnerabilities to DoS attacks in 802.11 networks”, Wireless Netw, pp.159-169, 2008

[16] Anmol Sheth and Rechard Han, “An Implementation of Transmit Power Control in 802.11b Wireless Networks”, Technical Report CU-CS-934-02, August, 2002.

[17] Mark Briggs, “Dynamic Frequency Selection and the 5GHz Unlicensed Band”, Technical Report, Elliott Lab.

[18] Wullems, C.; Tham, K.; Smith, J.; Looi, M., "A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs", Wireless Telecommunications Symposium, *2004* , pp. 129-136, May 2004.

[19] Roaming and Mobility [Online]. Available: http://en.wikipedia.org/wiki/Wireless_LAN#Roaming

[20] IEEE 802.11 Services [Online]. Available: http://www.intelligraphics.com/introduction-ieee-80211

[21] Mustafa Ergen, “IEEE 802.11 Tutorial”, June, 2002.

[22] 802.11 MAC Layer Functions [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/1216351

[23] Logical Link Control Layer Functions [Online]. Available: http://answers.yahoo.com/question/index?qid=20080209225815AAcjg3Q

[24] Logical Link Control Layer Functions [Online]. Available: http://www.rigacci.org/docs/biblio/online/intro_to_networking/c5048.htm

[25] Manmath Narayan Sahoo, Pabitra Mohan Khilar, *"Survivability of IEEE 802.11 Wireless LAN Against AP Failure"*, International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), pp.424-428, April, 2009.

[26] Jae Chung and Mark Claypool, *"ns by Example"*, Computer Science, Worcestor Polytechnic Institute [Online]. Available : http://nile.wpi.edu/NS/

[27] Kevin Fall and Kannan Varadhan, "The *ns* Manual", The VINT Project, January 6, 2009.

[28] Marc Greis, Tutorial for network simulator "ns" [Online]. Available: http://www.isi.edu/nsnam/ns/tutorial/index.html